локального оптимума. Вероятность мутации меняется в зависимости от количества поколений. В начале алгоритма вероятность мутаций выше, при схождении – ниже.

Применение генетического алгоритма для анализа графа атак, описывающего облачную инфраструктуру, позволяет значительно повысить защищенность системы при минимальном использовании ресурсов.

Библиографические ссылки

1. *Емельянова Ю. Г., Фраленко В. П.* Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления // Программные системы: теория и приложения : электрон. науч. журн. 2011. № 4(8). С. 17–31 [Электронный ресурс]. URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf

2. *Паюсова Т. И.* Анализ графа атак с помощью генетического алгоритма с переменной, вероятность мутации для предотвращения сетевых атак на облачные вычисления // Безопасность информационного пространства : сб. ст. Тюмень : Изд-во ТюмГУ, 2012. С. 112–116.

3. http://www.moysklad.ru/chto_takoe_oblachnye_servisy/

4. http://clouds-microsoft.blogspot.ru/p/blog-page_10.html

5. http://www.anti-malware.ru/node/2333

6. http://www.securitylab.ru/news/363719.php

СИСТЕМА ЭМУЛЯЦИИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Е. Ф. Попов
(Тюмень, ТюмГУ)

Динамичное развитие технологий передачи данных приводит к изменению угроз информационной безопасности. Появление новых методов атаки на сети передачи данных требует постоянного усовершенствования средств защиты информации.

При разработке программного обеспечения или проектировке систем, предназначенных для обеспечения информационной безопасности, важным этапом является тестирование выбранного или

разработанного решения. Тестирование зачастую производится в условиях, значительно отличающихся от реальных, а тестирование в рамках реальной информационной инфраструктуры осложняется опасностью воздействия на бизнес-процессы компании.

Для упрощения процесса тестирования средств обеспечения информационной безопасности планируется разработать систему эмуляции, способную создать виртуальную копию информационной инфраструктуры реальной компании, интегрировать в нее необходимые средства обеспечения информационной безопасности и произвести тестирование с использованием искусственно созданных атак, способных привести к инциденту информационной безопасности в данной инфраструктуре.

Основной задачей разработанной системы является создание виртуальных копий сетевых инфраструктур большого размера. Эмуляция десятков сетевых устройств требует вычислительных мощностей, которые не может обеспечить один сервер, что влечет за собой необходимость распределения нагрузки на кластер. Распределение нагрузки реализовано за счет разделения одной общей сетевой инфраструктуры на несколько сегментов, каждый из которых эмулируется на отдельном сервере. Связь сегментов обеспечивается за счет виртуальных транспортных магистралей так, что сетевые устройства не отличают подключения в рамках виртуального сегмента и подключения через виртуальную транспортную магистраль.

В любой сетевой инфраструктуре подключение устройств происходит через специальные каналы передачи данных, которые не требуют прямого взаимодействия операционных систем сетевых устройств между собой, а обеспечивают стандартизированную среду передачи. Наличие каналов передачи данных, которые являются посредниками во взаимодействии сетевых устройств, исключает необходимость эмуляции всех сетевых устройств на одном сервере.

Используемая система эмуляции обеспечивает передачу данных за счет перемещения пакета данных из области памяти, выделенной для буфера исходящих пакетов интерфейса сетевого устройства, с которого передаются данные, в область памяти, выделенную для буфера входящих пакетов интерфейса сетевого устройства,

которому предназначены данные. Формат и размер пакета данных зависят от типа интерфейса и используемого протокола передачи данных, которые являются стандартизированными и могут быть учтены в процессе разработки виртуальных транспортных магистралей.

Помимо подключения виртуальных сетевых устройств, виртуальные транспортные магистрали могут обеспечивать подключение между любыми виртуальными устройствами. С использованием систем виртуализации можно создать виртуальную копию реального сервера и подключить его к одному из виртуальных сетевых устройств через транспортную магистраль. Возможность использования различных систем виртуализации увеличивает степень соответствия создаваемых копий информационных инфраструктур реальным сетям, что позволяет производить тестирование средств обеспечения информационной безопасности с учетом не только сетевых устройств, но и серверной инфраструктуры.

Отметим, что имеется технологическая возможность подключения к эмулируемой сети не только виртуальных устройств, но и реальных, что позволяет, например, более точно прогнозировать последствия модернизации реальных инфраструктур.

Для упрощения начальной настройки и поддержки системы эмуляции разработана подсистема управления, которая разделена на клиентскую и серверную части. Серверная часть хранит конфигурации всех серверов, задействованных в эмуляции (далее ноды) и передает клиентскому приложению инструкции по изменению конфигураций. Клиентское приложение позволяет автоматически получать конфигурацию сегмента виртуальной сетевой инфраструктуры и вносить изменения в работу системы эмуляции. Для включения ноды в кластер достаточно установить клиентское приложение, которое развернет эмуляцию необходимого сегмента сети по запросу центрального сервера. Такая схема управления позволяет быстро развернуть виртуальную сетевую инфраструктуру на новом оборудовании.

Центральный сервер при подобной схеме не несет серьезных нагрузок, так как в штатном режиме производится только провер-

ка состояния нод, которая не является ресурсоемкой, а изменение конфигураций является относительно редким и генерирует лишь кратковременные нагрузки. Таким образом, каждый клиент, участвующий в эмуляции, несет нагрузки, связанные только с эмуляцией собственных устройств и передачей данных на ноды, с которыми существует связь с помощью виртуальных транспортных магистралей, а центральный сервер выполняет роль передатчика конфигураций, а также «мониторит» состояния нод.

Наличие единой точки управления всей распределенной системой эмуляции значительно упрощает администрирование. Помимо этого, существует потенциал автоматизации настройки всей системы эмуляции. Доработка подсистемы управления может обеспечить полностью автоматическое создание конфигураций для нод и распределение нагрузки. Например, нам необходимо эмулировать сеть из 40 маршрутизаторов, подключенных по топологии кольца, при условии, что у нас есть 15 компьютеров, обладающих разными характеристиками, на которых уже установлено клиентское приложение. Для поддержки интеллектуального распределения нагрузки клиентское приложение с каждой ноды передает серверу управления информацию о вычислительной мощности центрального процессора. Обладая данными о вычислительных мощностях всех нод, сервер автоматически распределяет виртуальные устройства по нодам, эмулируя на самых мощных компьютерах самое большое количество устройств. После распределения устройств генерируются настройки для внутренней системы эмуляции каждой ноды и настройки виртуальных транспортных магистралей, которые объединяют все сегменты в единую сеть.

Технологическая возможность подключения к виртуальной информационной инфраструктуре реальных устройств значительно упрощает не только создание копии реальной инфраструктуры, но и процесс имитации атак, в которых могут применяться специализированные аппаратные или программные средства. В результате данная система эмуляции позволяет проводить различные тесты защищенности информационной системы и эффективности средств защиты информации без воздействия на состояние реальной информационной инфраструктуры.